Abstract

SYSTEM, METHOD AND PROGRAM PRODUCT FOR DETECTING UNKNOWN COMPUTER ATTACKS

A computer system and program product for automatically determining if a packet is a new, exploit candidate. First program instructions determine if the packet is a known exploit or portion thereof. Second program instructions determine if the packet is network broadcast traffic presumed to be harmless. Third program instructions determine if the packet is network administration traffic. If the packet is a known exploit or portion thereof, network broadcast traffic, or network administration traffic, the packet is not considered a new, exploit candidate. If the packet is not a known exploit or portion thereof, network broadcast traffic, or network administration traffic, the packet is an exploit candidate. Alternately, the first program instructions determine if the packet is a known exploit or portion thereof. The second program instructions determine if the packet is network broadcast traffic presumed to be harmless. Third program instructions determine if the packet is another type presumed or known from experience to be harmless. If the packet is a known exploit or portion thereof, network broadcast traffic, or the other type, the packet is not considered a new, exploit candidate. If the packet is not a known exploit or portion thereof, network broadcast traffic, or the other type, the packet is an exploit candidate.